

Trend Micro ServerProtect™ for Linux

CentOS / Suse 11



クイックスタートガイド

安心を、ひとつ上のステージへ。



※注意事項

トレンドマイクロへのお客様情報の送信について

- 「Webレピュテーションサービス」「フィッシング詐欺対策」「有害サイト規制/URLフィルタリング」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化してトレンドマイクロのサーバに送信します。サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。また、これらの機能を有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがあります。
 - (a)お客様がアクセスしたWebページのWebサーバ側の仕様が、お客様が入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客様の入力した情報(ID、パスワード等)などを含んだURLがトレンドマイクロのサーバに送信される。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。
- 「ファイルレピュテーションサービス」では、ファイルの安全性の判定のために、ファイルのハッシュ値等の情報をトレンドマイクロのサーバに送信します。ファイルそのものや、ファイルの内容に関する情報は送信しません。
- 「ソフトウェア安全性評価サービス/脅威情報の送信」では、プログラムの安全性の判定のために、プログラムまたはプログラムの情報をトレンドマイクロのサーバに送信します。
- 「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
- 「迷惑メール対策ツール」では、弊社製品の改良の目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- 「E-mailレピュテーションサービス」では、スパムメールの判定のために、送信元のメールサーバの情報をトレンドマイクロのサーバに送信します。
- 「スマートフィードバック」では、脅威に関する情報を収集、分析し保護を強化するために、不正な動きをする可能性があるトレンドマイクロが判断したファイル、ファイルのチェックサム、アクセスされたWebアドレス、サイズやパス等のファイル情報、実行ファイルの名前等の情報をトレンドマイクロのサーバに送信します。送信されたファイルはプログラムの安全性の判定のために利用されます。またファイルにお客さまの個人情報や機密情報等が意図せず含まれる可能性があります。トレンドマイクロがファイルに含まれる個人情報や機密情報自体を収集または利用することはありません。お客さまから収集された情報の取り扱いについての詳細は、<<http://jp.trendmicro.com/jp/about/privacy/spn/index.html>>をご覧ください。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のWebサイトから見つけることができます。「<http://www.treas.gov/offices/enforcement/ofac/>」および「<http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.html>」
2009年7月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。
あなたは本製品に関連した米国輸出管理法の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

- お客様が複数年契約(複数年分のサポート費用前払い)された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認ください。
<http://jp.trendmicro.com/jp/support/lifecycle/index.html>

著作権について

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trend プロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、Smart Protection Network、SPN、および SMARTSCANは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright ©2001-2010 Trend Micro Incorporated. All rights reserved.

P/N: SPLXFF-AE0200_R2_CentOS (2010/06)

目次

はじめに	7
対象読者	8
ドキュメント	8
ドキュメントの表記規則	9
第 1 章 インストールの準備	11
システム要件	12
ServerProtect のインストールに必要な情報	15
第 2 章 インストール	17
ServerProtect インストーラオプション	18
ローカルインストールの手順	19
インストールプログラムを実行する	19
トレンドマイクロのエンドユーザ使用許諾契約書に同意する	21
ServerProtect を Control Manager に登録する	21
インストール時にアクティベートする	24
ウイルストラッキングオプションを指定する	25
リモートインストール	26
RemotelInstall を ServerProtect のバイナリから抽出する	27
リモート配信で設定ファイルを使用する	28
RemotelInstall ツールを実行する	31
カーネルフックモジュール	34
カーネルフックモジュールをインストールする	35
インストールを確認する	37

ServerProtect をアンインストールする	37
第 3 章 インストール後の設定	39
ServerProtect Web コンソールにログオンする	40
Java プラグインを有効にする	42
管理者パスワードを設定する	42
プロキシサーバを設定する	43
一般的なプロキシ設定	43
コンポーネントアップデートでのプロキシの設定	44
ServerProtect を登録する	46
アクティベーションを実行する	47
製品版にアップグレードする	49
コンポーネントをアップデートする	51
Control Manager による自動アップデートの開始	51
EICAR テストウイルスを使用して ServerProtect をテストする	52
SUSE Linux の syslog-ng を設定する	53
付録 A カーネルフックモジュールの構築とインストール	55
はじめに	56
要件	56
インストール	57
付録 B トラブルシューティングとテクニカルサポート	65
トラブルシューティング	66
64 ビット SUSE Linux 上でのインストールに関連する問題	66
Linux 内で、依存ライブラリがないことに関連する問題	66
KHM の構築とインストール	67

初期設定のパスワード	70
Web コンソールでパスワードが拒否される	70
デバッグログ	71
お問い合わせいただく前に	71
製品サポート情報	72
サポートサービスについて	72
製品 Q&A のご案内	73
セキュリティ情報	73
セキュリティ情報の入手先	73
トレンドマイクロへのウイルス解析依頼	74
ウイルス解析サポートセンター「TrendLabs」	75
ソフトウェアアップデートについて	75
既知の問題	76
索引	79

はじめに

Trend Micro ServerProtect for Linux (以下、ServerProtect) クイックスタートガイドをお読みいただき、ありがとうございます。本書では、ServerProtect のインストールに必要となる作業内容および基本的な設定について説明します。本章では、次の内容について説明します。

- 8 ページの「対象読者」
- 8 ページの「ドキュメント」
- 9 ページの「ドキュメントの表記規則」

対象読者

本書の読者は、次の内容を含め、中級から上級レベルの Linux システム管理についての知識を持っていることを前提としています。

- Linux サーバのインストールおよび設定
- Linux サーバでのソフトウェアのインストール
- ネットワークの概要 (IP アドレス、ネットマスク、トポロジー、LAN 設定など)
- さまざまなネットワークトポロジー
- ネットワークデバイスおよびその管理方法
- ネットワーク構成 (VLAN、SNMP、SMTP などの使用)

ドキュメント

ServerProtect には、次のようなドキュメントが付属しています。

- **管理者ガイド** — このガイドは、ServerProtect の特長や機能について説明しています。製品の設定や管理についてサポートします。また、有用な付録や用語集なども用意されています。
- **クイックスタートガイド (本書)** — このガイドは、ServerProtect を紹介し、インストールの計画および実行をサポートすることで、ServerProtect の使用法を習得することを支援します。また、安全なテスト用ウイルスを使用して、インストール内容をテストする方法も説明しています。
- **オンラインヘルプ** — オンラインヘルプの目的は、製品の主要タスクの実行方法を説明し、使用上のアドバイスを提示し、有効なパラメータ範囲や最適値などの入力フィールド情報を提供することです。オンラインヘルプには、ServerProtect の管理コンソールからアクセスできます。
- **man ページ (マニュアルページ)** — ServerProtect には、`splxmain`、`splx`、`tmsplx.xml`、`RemotelInstall`、および `CMconfig` のファイルに関する man ページが用意されています。

-
- **Readme ファイル** — Readme ファイルには、オンラインドキュメントや印刷版ドキュメントには記載されていない最新の製品情報が記載されています。たとえば、新機能の説明、インストールに関するヒント、既知の問題、リリース履歴などが記載されています。
 - **製品 Q&A** — 製品 Q&A は、問題の解決方法やトラブルシューティングの情報が格納されたオンラインデータベースです。製品 Q&A では、製品の既知の問題に関する最新情報が提供されます。製品 Q&A には、次の URL からアクセスできます。

<http://esupport.trendmicro.co.jp/>

ヒント：トレンドマイクロでは、最新版ダウンロードサイト (<http://www.trendmicro.co.jp/download/>) から対応するリンクをクリックして、製品ドキュメントの最新版を入手することをお勧めします。

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、ドキュメントでは、次の表記規則を使用しています。

表記	説明
注意：	設定上の注意
ヒント：	推奨事項
警告：	避けるべき操作や設定についての注意

表 1. 本書で使用している表記規則

インストールの準備

本章では、Trend Micro ServerProtect for Linux (以下、ServerProtect) の Linux サーバへのインストール前の情報収集の段階について説明します。

本章では、次の内容について説明します。

- 12 ページの「システム要件」
- 15 ページの「ServerProtect のインストールに必要な情報」

システム要件

ServerProtect をインストールするには、次の要件を満たしている必要があります。

ハードウェア

プロセッサ

- Intel Pentium II 以上
- AMD Athlon 以上

注意：本バージョンの ServerProtect は、Intel 64 アーキテクチャを使用した Intel プロセッサ、および AMD 64 テクノロジーを使用した AMD プロセッサをサポートしています。Intel Itanium アーキテクチャはサポートされていません。

メモリ

- 512MB 以上 (アプリケーションサーバ/ファイルサーバには 1GB 推奨)

ハードディスク空き容量

- 250MB (/opt ディレクトリで使用)
- 250MB (/tmp ディレクトリで使用)

ソフトウェア

対応ディストリビューションおよびカーネル

- SUSE Linux Enterprise 11 (Server または Desktop) (i686 および x86_64)
 - 2.6.27.42-0.1.1-default i686
 - 2.6.27.42-0.1.1-pae i686
 - 2.6.27.42-0.1.1-xen i686
 - 2.6.27.42-0.1.1-default x86_64
 - 2.6.27.42-0.1.1-xen x86_64
- CentOS 4 (i686 および x86_64)
 - 2.6.9-89.0.19.EL i686
 - 2.6.9-89.0.19.ELsmp i686
 - 2.6.9-89.0.19.EL x86_64
 - 2.6.9-89.0.19.ELsmp x86_64
- CentOS 5 (i686 および x86_64)
 - 2.6.18-164.11.1.el5 i686
 - 2.6.18-164.11.1.el5PAE i686
 - 2.6.18-164.11.1.el5xen i686
 - 2.6.18-164.11.1.el5 x86_64
 - 2.6.18-164.11.1.el5xen x86_64

カーネルのサポートに関する最新情報については、次のトレンドマイクロ Web サイトで提供しています。

<http://www.trendmicro.co.jp/download/kernel.asp?productid=20>

Fault Tolerant サーバ

- NEC ft サーバ Express5800 / 320Fb-L, 320Fb-LR (MIRACLE LINUX 対応モデル)

対応 X Window グラフィカルデスクトップ環境

Quick Access コンソールメニューを使用するには、Konqueror Desktop Environment (KDE) 3.3 以上をインストールします。

注意： Quick Access コンソールは、root でログオンした場合のみ使用可能です。

対応 Web ブラウザ

ServerProtect Web コンソールへは、次のいずれかからアクセスします。

- Microsoft Internet Explorer 5.5 Service Pack 2 以上

注意： Internet Explorer 7.0 をお使いの場合、Web コンソールのオンラインヘルプの内容を表示するには、ポップアップウィンドウのブロック機能を無効にする必要があります。

- Mozilla 1.7 以上 — Java Runtime Environment (JRE) 1.4.2_01 以上 (バージョン 1.5.0_02 まで) が必要です。
- Mozilla Firefox 1.0 以上 — Java 2 Runtime Environment 1.4.2_01 以上 (バージョン 1.5.0_02 まで) が必要です。

注意： システム要件に記載されているオペレーティングシステムの種類やハードディスク容量などは、本ドキュメント作成時点の情報です。システム要件は、オペレーティングシステムのサポート終了や、弊社製品の改良、検索エンジンやパターンファイルのバージョンアップなどに伴い、変更、追加、または削除される場合があります。また、製品の運用環境によっては、ログファイルの保存、他のソフトウェアとの共存などにより、必要となるメモリサイズやハードディスク容量も異なりますので、ご注意ください。最新のシステム要件については、弊社 Web サイトのサポートページやサポート窓口でご確認ください。

ServerProtect のインストールに必要な情報

ServerProtect のセットアッププログラムでは、インストールプロセス時に選択したオプションに応じて、必要な情報を入力するようにポップアップが表示されます。

インターネットのアップデート用プロキシ

ServerProtect サーバとインターネット間にプロキシがある場合、プロキシのホスト名または IP アドレス、ユーザ名、およびパスワードを入力します。

Trend Micro Control Manager サーバ情報

ServerProtect を既存の Trend Micro Control Manager (以下、Control Manager) サーバに登録する場合、そのサーバのホスト名または IP アドレス、およびログオン名が必要です。

注意： ServerProtect をお使いのネットワーク上の Control Manager サーバに登録するには、Control Manager サーバ 3.5 Patch 3 以上が必要です。

アクティベーションコード

製品の登録時に、レジストレーションキーと引き換えにアクティベーションコード / シリアル番号を取得し、プログラムの「ロックを解除」します。次のトレンドマイクロのオンライン登録 Web サイトにアクセスして、インストール前にアクティベーションコードを登録し、取得できます。

<https://olr.trendmicro.com/registration/jp/ja/login.aspx>

注意：すでにアクティベーションコードをお持ちの場合には、オンライン登録の必要はありません。アクティベーションコードの詳細については、販売代理店にお問い合わせください。

ローカルまたはリモートインストール

本バージョンの ServerProtect は、ローカルサーバまたはリモートサーバのいずれにもインストールできます。また、1 台でも、複数のリモートサーバでもインストールできます。

インストール

本章では、Linux サーバへの Trend Micro ServerProtect for Linux (以下、ServerProtect) のインストールを説明します。本章では、次の内容について説明します。

- 18 ページの「ServerProtect インストーラオプション」
- 19 ページの「ローカルインストールの手順」
- 26 ページの「リモートインストール」
- 34 ページの「カーネルフックモジュール」
- 37 ページの「インストールを確認する」

ServerProtect インストーラオプション

インストーラで使用できるパラメータの詳細を表示するには、次のコマンドを実行してください。

```
./SPprotectLinux-3.0.bin -h
```

次の表では、パラメータについて説明します。

オプション	説明
-f RedHat SuSE i686 x86_64	指定されたディストリビューション向けの ServerProtect を強制的にインストールします。
-h	このバイナリ (現在表示している出力) で使用可能なパラメータのリストを表示します。
-n	ServerProtect をインストールした後に、ServerProtect サービスを開始しません。
-r	リモートインストールツールを抽出します。
-s	使用許諾契約書を表示しません。
-S {アクティベーションコード}	アクティベーションコードを入力して、ServerProtect をアクティベートします。
-x	ServerProtect の rpm ファイルを抽出します。
-X RedHat SuSE i686 x86_64	指定されたディストリビューション向けの ServerProtect のバイナリファイルを抽出します。
-w {yes/no}	ウイルストラッキングプログラムへ情報を送信するかどうかを設定します。

注意： このスクリプトでは、CentOS に RedHat が使用されます。

ローカルインストールの手順

次のリストでは、ローカルの Linux サーバでの ServerProtect のインストール手順を示します。それに続くセクションでは、この手順について詳細に説明します。

- 手順 1: 「インストールプログラムを実行する」
- 手順 2: 「トレンドマイクロのエンドユーザ使用許諾契約書に同意する」
- 手順 3: 「ServerProtect を Control Manager に登録する」
- 手順 4: 「インストール時にアクティベートする」
- 手順 5: 「ウイルストラッキングオプションを指定する」
- 手順 6: 「カーネルフックモジュールをインストールする」(必要に応じて)

インストールプログラムを実行する

ServerProtect をインストールする前に、お使いの Linux のディストリビューションとカーネルがこのリリースでサポートされていることを確認してください (13 ページの「対応ディストリビューションおよびカーネル」を参照)。お使いのカーネルが「システム要件」セクションに記載されていない場合は、「カーネルフックモジュールをインストールする」セクションの手順に従って、お使いの Linux システムに対応したカーネルフックモジュール (以下、KHM) を入手していただく必要があります。

注意: Linux コンピュータに ServerProtect を正常にインストールする前に、次の依存ライブラリをインストールするようにします。

- gtk2
 - pango
 - atk
-

ServerProtect インストールを開始するには

1. ServerProtect のインストールファイルをダウンロードまたはコピーします。
2. root でログオンします。

3. ServerProtect のインストールファイルが含まれるディレクトリで、次のコマンドを実行します。

```
./SProtectLinux-3.0.bin
```

このコマンドを実行すると、必要なファイルが適切な場所に抽出されます。次の手順では、インストール時にリアルタイム検索を無効にする方法を説明します。

リアルタイム検索を無効にして ServerProtect をインストールするには

1. `-n` オプションを使用して、インストールを開始します。たとえば、`./SProtectLinux-3.0.bin -n` のコマンドを実行します。
2. インストールが完了したら、`tmsplx.xml` 設定ファイルの `RealtimeScan` パラメータの値を「0」に設定します。
3. ServerProtect サービスを再起動します。

注意： KHM がお使いの Linux カーネルをサポートしていないという警告メッセージが表示された場合、KHM を構築してインストールします。KHM のインストールが完了しても、ServerProtect サービスを起動、または再起動しないでください。次に、上記の手順 2 および 3 を実行します。

警告： `-n` オプションを使用して ServerProtect をインストールする場合、システムスタートアップで実行するには、ServerProtect サービスを手動で設定する必要があります。そのためには、`/opt/TrendMicro/SProtectLinux/SPLX.util` フォルダで「`./add_splx_service`」を実行します。

トレンドマイクロのエンドユーザ使用許諾契約書に同意する

ServerProtect のインストールを開始する前に、製品に同梱されている使用許諾契約書を読んでください。

注意： 製品の使用にあたってはインストール時に表示される英語の許諾契約書は適用されず、製品に同梱されている日本語の許諾契約書が適用されます。

スペースキーを押して、使用許諾契約書をスクロールします。最後に「yes」と入力してください（「yes」を入力しない場合は、インストールを続行できません）。

NOTICE:Trend Micro licenses its products in accordance with certain terms and conditions.By breaking the seal on the CD jacket in the Software package or installing a serial number, registration key or activation code, You already accepted a Trend Micro license agreement.A courtesy copy of a representative Trend Micro License Agreement is included for reference below.The language and terms of the actual Trend Micro license agreement that you accepted may vary.By accepting the License Agreement below, or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

Trend Micro License Agreement
(Package Version 0403Nov03E021004)

-----[SNIP]-----

SPLX version 3.0 Released June 29, 2007

Do you agree to the above license terms?(yes or no)

図 2-1. インストール時に表示される使用許諾契約書画面（表示例）

ServerProtect を Control Manager に登録する

Control Manager を使用して ServerProtect を管理する場合は、インストール時に ServerProtect を Control Manager に登録できます。

ServerProtect を Control Manager に登録するには

1. 19 ページの「ServerProtect インストールを開始するには」の手順に従って、ServerProtect のインストールを開始します。
2. 「Do you wish to connect this SPLX server to Trend Micro Control Manager?」というメッセージが表示されたら、「y」と入力して <Enter> キーを押します (または単に <Enter> キーを押して初期設定の「y」を選択します)。ユーザから必要なデータを収集することを通知するメッセージが表示されて、ServerProtect サーバ用に使用できる IP アドレスのリストが表示されます。
Control Manager を使用して ServerProtect を管理しない場合は、「n」と入力して <Enter> キーを押します。「Activate ServerProtect to continue scanning and security updates.」というメッセージが表示され、アクティベーションコードの入力のためのプロンプトが表示されます。このプロセスの詳細については、24 ページの「インストール時にアクティベートする」を参照してください。
3. 「SPLX server name or IP address」プロンプトで、ServerProtect サーバの名前または IP アドレスを入力します。
4. 「Do you wish to connect to Control Manager server using HTTPS?(y/n) [n]」プロンプトで、HTTPS を使用して Control Manager に接続する場合には「y」を、HTTP 接続を使用する場合には「n」を入力します。
5. 「Control Manager server name or IP address:」プロンプトで、ServerProtect を管理するための Control Manager サーバのサーバ名または IP アドレスを入力します。
6. 「Control Manager server port:[80]」プロンプトで、Control Manager にアクセスするためのポートの番号を入力するか、単に <Enter> キーを押して初期設定値の 80 を選択します。
7. 「Do you access Control Manager through a proxy server?(y/n) [n]」プロンプトで、「y」を入力するか (yes の場合)、単に <Enter> キーを押して初期設定の「n」を選択します。「n」を選択した場合は、Control Manager の Web コンソールで ServerProtect を識別するための表示名を指定するように要求されます。プロキシサーバを使用して Control Manager に接続する場合は、23 ページの「プロキシサーバの情報」を参照してこのプロセスの詳細を確認してください。

8. 「Please specify the name you would like to display on the Control Manager console:[SPLX server name or IP address]」プロンプトで、適切な名前を入力します。Control Manager は、この名前を使用して Control Manager の Web コンソール上で ServerProtect サーバを識別します。
9. 「Please specify a folder name for this product (for example:/SPLX) [New entity]:」プロンプトで、ServerProtect を登録する Control Manager の製品ディレクトリ上のフォルダパスを入力します (この入力を省略して <Enter> キーを押した場合、「新規エンティティ」フォルダに登録されます)。ユーザが入力した情報が一覧表示されて、選択内容を確認するように要求されます。
10. 「Is the above information correct? (y/n) [n]」プロンプトで、表示された選択内容が正しいかどうかを確認します。「n」と入力するか、単に <Enter> キーを押して初期設定の「n」を選択した場合は、ServerProtect サーバの IP アドレスから始まる前述のすべての情報を再入力するためのプロンプトが表示されます。「y」と入力してすべての表示された情報を確定した場合は、「Saving information to the configuration file done」というメッセージが表示されて、アクティベーションコードを入力するかどうか尋ねられます。このプロセスの詳細については、24 ページの「インストール時にアクティベートする」を参照してください。

プロキシサーバの情報

プロキシサーバを使用して Control Manager に接続する場合は、インストール時にプロキシサーバの情報を入力して、ServerProtect が Control Manager と正しく通信できるようにしてください。

インストール時にプロキシサーバの情報を指定するには

以下のプロンプトで該当する情報を入力してください。

- Proxy Server name or IP address:(プロキシサーバの名前または IP アドレス)
- Proxy Server port: [80](プロキシサーバのポート番号)
- Does your proxy server require user authentication? (y/n) [n](プロキシサーバでユーザ認証が必要かどうか)
(認証が必要な場合)

- Proxy user name:(プロキシのユーザ名)
- Proxy password:(プロキシのパスワード)
- Retype proxy password:(プロキシのパスワードの確認入力)

インストール時にアクティベートする

アクティベートした場合は、製品版の製品がインストールされます。これを省略すると、ServerProtect はアクティベートされず、検索機能およびコンポーネントのアップデート機能は有効になりません。アップデートは、ServerProtect をアクティベートするまで再開されません。

1. ServerProtect を登録するためのプロンプトが表示されます。アクティベーションコードをすでに取得している場合は手順 2 に進んでください。

<p>Step 1. Register Use the Registration Key that came with your product to register online (https://olr.trendmicro.com/redirect/product_register.aspx) . (Please skip this step if the product is already registered.)</p> <p>Step 2. Activate Type the Activation Code received after registration to activate ServerProtect. (Press [Ctrl+D] to abort activation.)</p>

図 2-2. インストール時に ServerProtect を登録するためのプロンプト

- a. 今すぐ登録するには、次の URL にアクセスします。

<https://olr.trendmicro.com/registration/jp/ja/login.aspx>

- b. 46 ページの「ServerProtect を登録する」に示された手順に従います。

2. 次に、ServerProtect をアクティベートするためのプロンプトが表示されます。この時点でアクティベートすることも、この手順を省略して後でアクティベートすることもできます。この手順を省略する場合は、<Ctrl>+<D> キーを押します。

ServerProtect をアクティベートするには、アクティベーションコードをプロンプトに入力して、<Enter> キーを押します。

インストール時に登録またはアクティベーションを実行しなかった場合の ServerProtect の登録手順は、46 ページの「ServerProtect を登録する」を参照。

ウイルストラッキングオプションを指定する

プロンプトが表示され、ウイルストラッキングプログラムに参加するかどうか尋ねられます。この設定の変更は、後で ServerProtect Web コンソールからいつでも選択できます。

World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map (<http://www.trendmicro.com/map>). Use this map to view virus trends for each continent and selected countries.

Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, aggregated detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program. It will not send out company names, individual names, machine names, site names, IP addresses, or any other identifying information. I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

No, I don't want to participate.
Please input your choice [Yes]:

(日本語訳)
ウイルストラッキングプログラム

トレンドマイクロでは、世界各国で実施されたウイルス検索の結果を収集し、統計情報をリアルタイムで提供しています。この情報は、トレンドマイクロウイルストラッキングセンター (<http://wtc.trendmicro.com/japanese/>) で参照することができます。ウイルストラッキングセンターでは、世界で流行しているウイルスや、選択した地域別の情報を得ることができます。

Yes - 私はウイルストラッキングプログラムに参加します。システムでウイルスが検出されたときにウイルス名や検出数などの情報がウイルストラッキングセンターに送信されること、企業名や個人名、コンピュータ名、サイト名、IP アドレスなどのその他の情報は送信されないこと、製品コンソール内で設定を [No] に変更すればいつでもこの自動レポート機能を無効にできることを私は了解しています。

No - 私はウイルストラッキングプログラムに参加しません。

オプションを選択してください [初期設定: Yes]:

図 2-3. ウイルストラッキングプログラムのオプション

リモートインストール

集中管理された分散環境に ServerProtect をインストールして管理できるようにするために、リモートインストールツール(RemoteInstall) を提供しています。

RemoteInstall の機能

RemoteInstall には次の機能があります。

- ServerProtect をリモートコンピュータにインストールします。
- 設定ファイルにはクライアントコンピュータのアカウント情報が保持されます。
- ServerProtect のインストール後に、ServerProtect の設定データを対象コンピュータに配信します。
- ServerProtect のインストール後に、カーネルフックモジュール (KHM) を対象コンピュータに配信します。
- クライアント環境に関する特定の情報を収集します (実行している Linux ディストリビューションや Linux カーネル番号など)。
- 設定情報を .CSV 形式でエクスポートできます。これにより RemoteInstall は、初回の配信が失敗したコンピュータのリストをそれ以降の配信で再利用します。

リモートインストールの実行手順は、次のとおりです。

1. RemoteInstall の抽出
2. RemoteInstall 設定ファイルの編集
3. RemoteInstall の実行

RemoteInstall を ServerProtect のバイナリから抽出する

-r パラメータを使用して、RemoteInstall を単一パッケージから、または特定の Linux カーネルバージョン用のバイナリファイルから抽出できます。たとえば、次のコマンドを実行すると、ServerProtect のバイナリファイルからリモートインストールツールが抽出されます。

```
./SPProtectLinux-3.0.bin -r
```

使用許諾契約書に同意して、リモートインストールプログラム (RemoteInstall) を抽出した後で、上記のコマンドを実行すると、作業ディレクトリの下に `remote.install.splx` サブディレクトリが作成されます。このサブディレクトリに含まれるファイルとディレクトリのリストについては、次の表を参照してください。

ファイルまたはディレクトリ	説明
config/	ServerProtect の設定ファイルの配信用のディレクトリ。次の 4 つのファイルが含まれます。 <ul style="list-style-type: none">• <code>tmsplx.xml</code> — ServerProtect の設定ファイル。このファイルを配信用に変更できます。• <code>tmsplx.xml.template</code> — 上記設定ファイルのテンプレートファイル (<code>tmsplx.xml</code>)。 <code>tmsplx.xml</code> が壊れた場合は、このテンプレートを使用してこのファイルを復元できます。• <code>xmldeployer</code> — 設定ファイル配信用のスクリプト。• <code>xmlvalidator</code> — <code>tmsplx.xml</code> 内のすべてのキーの値を検証するためのツール。
KHM.module/	KHM ファイル配信用のディレクトリ
RemoteInstall	リモートインストールツール
RemoteInstall.conf	配信用の設定ファイル
RemoteInstall.csv	.CSV 形式のファイルを .conf 形式に変換するためのテンプレート

表 2-1. RemoteInstall のディレクトリ

リモート配信で設定ファイルを使用する

RemoteInstall で使用される初期設定の設定ファイルは、**RemotelInstall.conf** です。抽出時に、このファイルは **remote.install.splx** ディレクトリに配置されています。

RemotelInstall.conf は、多くのキーが含まれた複雑な設定ファイルです。この設定ファイルは、次の 3 種類の配信で使用できます。

1. ServerProtect パッケージの配信とインストール
2. ServerProtect の設定のアップデート
3. カーネルフックモジュール (KHM) の配信

次の表では最も重要な設定可能キーのみを示しています。キーの詳細については、「管理者ガイド」を参照してください。

キー	説明
DeployOption	実行する配信の種類を指定します。 1 : ServerProtect パッケージの配信とインストール 2 : ServerProtect の設定ファイルのアップデート 3 : KHM の配信
PackageName	パッケージ配信用の ServerProtect インストールパスを指定します
ActivationCode	パッケージ配信で使用されます。インストール用の ServerProtect のアクティベーションコードを指定します
ConfigFilePath	設定ファイルの配信で使用されます。設定ファイルのパスを指定します

表 2-2. 最もよく使用される RemotelInstall.conf の設定可能キー

CSV 形式のファイルを RemotelInstall.conf 形式に変換する

設定ファイルを簡単に変更できるように、RemoteInstall には、ファイルを CSV 形式でインポートするためのオプションが用意されています。設定ファイルの情報を表計算プログラム (OpenOffice に含まれるものなど) で変更する場合は、次の手順に従ってください。

RemoteInstall の設定ファイルを CSV 形式で編集および使用するには

1. RemoteInstall.csv ファイルを表計算プログラムにインポートして編集します。ファイルを別のファイル名で保存します。
2. この新しいファイルを ServerProtect の remote.install.splx ディレクトリにコピーします。
3. RemoteInstall を実行する際には、次の例のように -p オプションの後ろに変更後の CSV ファイルの名前を指定します。

```
./RemoteInstall -p my_conf_file.csv
```

RemoteInstall は、次の命名規則に従って CSV ファイルを RemoteInstall.conf 形式に変換します。RemoteInstall_yyyy-mm-dd_hhmmss.conf

リモート配信先のクライアントを指定する

RemoteInstall.conf の「Client assignment」セクションの情報を変更して、リモート配信先のクライアントを指定します。このセクションには、配信先のリモートコンピュータを指定するための 2 つのサブセクションがあります。RemoteInstall の配信先となる 1 台のコンピュータの設定を入力するには、「#single deploy」セクションを編集します。1 つ以上のクライアントグループの設定を入力するには、「#group deploy」セクションを編集します。1 回の配信で両方のセクションを使用することもできます。

以下では、正しく配信するために入力する必要のある設定データを一覧表記しています。

シングル配信

RemoteInstall.conf の「Client assignment」セクションの「#single deploy」には、正しく配信するために RemoteInstall が認識する必要のある 13 個の設定項目があります。

行	説明
1. [x.x.x.x]	クライアントの IP アドレス
2. RootPassword	クライアントの root パスワード

行	説明
3. ConnectCM	1 (初期設定) : Control Manager サーバに登録します。 0 : Control Manager サーバに登録しません。
4. CMServerIP	Control Manager サーバの IP アドレス
5. CMServerPort	Control Manager サーバの接続ポート (初期設定 =80)
6. UseProxyAccessCM	1 : プロキシサーバを使用して Control Manager サーバに接続します。 0 (初期設定) : プロキシを使用しません。
7. ProxyServerIP	プロキシサーバの IP アドレス
8. ProxyServerPort	プロキシサーバの接続ポート (初期設定 =80)
9. ProxyAuthentication	1 : プロキシ認証を使用します。 0 (初期設定) : プロキシ認証を使用しません。
10. ProxyUserName	プロキシ認証のユーザ名
11. ProxyPassword	プロキシ認証のパスワード
12. CMClientName	Control Manager コンソールに表示されるクライアントコンピュータ名 初期設定 = クライアントの IP アドレス
13. CMProductDirectoryName	Control Manager コンソールに表示されるディレクトリ名。ディレクトリを使用してクライアントがグループ分けされます。 初期設定 = 「新規エンティティ」

表 2-3. 設定ファイル内のクライアント割り当てキー (シングル配信)

グループ配信

グループ配信の場合は、次の表以外のすべての行は「#single deploy」と同じです。

行	説明
1. [Group1]	1 台のコンピュータの IP アドレスのキーの代わりに、最初のキーでは配信先クライアントのグループを指定します。
14. Machine1	この行（およびこの後に必要なだけ記述される行）では、RemoteInstall が ServerProtect を配信する各コンピュータの IP アドレスを列記します。
15. Machine2	(同上)
(必要なだけ記述)	(同上)

表 2-4. 設定ファイル内のクライアント割り当てキー（グループ配信）

ヒント：参照しやすいように、すべてのグループ名は、営業、研究開発のように分かりやすい語を先頭に付けることをお勧めします。同様にコンピュータ名も、Server1、Server2 のように指定することをお勧めします。

RemoteInstall ツールを実行する

下記の主要な手順に従って RemoteInstall プログラムを実行してください。

RemoteInstall を実行するには

1. ServerProtect のすべてのバイナリファイルを配信サーバに配置します。
2. RemoteInstall を ServerProtect のバイナリから抽出します（詳細については、27 ページの「RemoteInstall を ServerProtect のバイナリから抽出する」を参照してください）。

3. ServerProtect を複数のコンピュータに配信するには、**RemoteInstall.conf** を配信用に設定します(**RemoteInstall.conf** ファイルの詳細については、28 ページの「リモート配信で設定ファイルを使用する」を参照してください)。
4. 次のコマンドをコマンドラインから実行します。

```
./RemoteInstall
```

RemoteInstall は、ServerProtect を対象コンピュータに配信して、進行状況メッセージを出力します。この配信によって、次の表に示す 5 つの結果ファイルが作成されます。

結果ファイル	説明
splx_failed_list_yyyy-mm-dd_hhmmss.conf	設定ファイル形式の失敗リスト
splx_failed_list_yyyy-mm-dd_hhmmss.csv	.CSV ファイル形式の失敗リスト
splx_success_list_yyyy-mm-dd_hhmmss.conf	設定ファイル形式の成功リスト
splx_success_list_yyyy-mm-dd_hhmmss.csv	.CSV ファイル形式の成功リスト
splx_remote_status_yyyy-mm-dd_hhmmss.txt	配信ステータス

表 2-5. RemoteInstall によって作成される結果ファイル

RemoteInstall ツールのオプション

RemoteInstall ツールのオプションの使用方法を表示するには、次のように `-h` パラメータを使用してください。

```
./RemoteInstall -h
```

パラメータ	説明
<code>-c</code>	クライアント情報をチェックします。
<code>-f {代替設定ファイル}</code>	リモートインストールの設定ファイルを指定します。このオプションは、 RemoteInstall.conf 以外の設定ファイルを使用して RemoteInstall を実行する場合に使用します（代替設定ファイルを使用できるのは、この代替ファイルに RemoteInstall.conf と同じキー / 値ペアが含まれている場合のみです。28 ページの「リモート配信で設定ファイルを使用する」を参照してください）。
<code>-h</code>	使用方法を表示します。
<code>-n</code>	使用許諾書を表示しません。
<code>-p {CSV ファイル}</code>	指定した CSV ファイルを RemoteInstall で使用する設定ファイルに変換します（このオプションの詳細については、28 ページの「CSV 形式のファイルを RemoteInstall.conf 形式に変換する」を参照してください）。
<code>-v</code>	バージョンを表示します。

表 2-6. RemoteInstall スクリプトで使用できるパラメータ

カーネルフックモジュール

このバージョンの ServerProtect には、サポートされている各カーネル用のカーネルフックモジュール (KHM) が付属しています。KHM のソースコードも、インストールパッケージに含まれています。

ServerProtect でリアルタイム検索を実行するには、KHM をインストールする必要があります。お使いの Linux カーネルが、13 ページの「対応ディストリビューションおよびカーネル」のリストにある場合、ServerProtect セットアッププログラムにより、ServerProtect パッケージに付属する適切な KHM が自動的にインストールされています。

お使いの Linux カーネルがリストにない場合、次を実行します。

1. お使いの Linux カーネルに適した KHM を、次のトレンドマイクロ Web サイトからダウンロードします。

<http://www.trendmicro.co.jp/download/kernel.asp?productid=20>

2. お使いの Linux カーネルに適した KHM が使用できない場合、Linux システム上で KHM を構築します。構築手順は、55 ページの「カーネルフックモジュールの構築とインストール」を参照してください

注意： Linux カーネルをアップグレードする際には、KHM を ServerProtect のインストール先ディレクトリにコピーする必要があります。

カーネルフックモジュールをインストールする

本セクションでは、トレンドマイクロ Web サイトからダウンロードした KHM パッケージのインストール方法を説明します。また、ServerProtect のインストール後、最新の KHM をインストールすることもできます。

注意： インストール中に、インストールを続行するには依存パッケージのインストールが必要であるというエラーメッセージが表示された場合は、お使いの Linux システムに対応した KHM を上記のトレンドマイクロ Web サイトから入手してください。

KHM をインストールするには

1. root でログオンします。
2. お使いのカーネルが最新バージョンの ServerProtect でサポートされていることを確認するには、次の URL にアクセスします。

<http://jp.trendmicro.com/jp/products/enterprise/sp-linux/index.html>

3. KHM の名前は、対応するカーネルバージョンに応じて付けられます。お使いの Linux カーネルに適した KHM パッケージをダウンロードして、次のディレクトリにコピーします。

`/opt/TrendMicro/SProtectLinux/SPLX.module/`

4. 上記のディレクトリに移動して、次のコマンドを実行して KHM パッケージを抽出します。

```
tar xzvf {SPLX バージョンとカーネルバージョン}.tar.gz
```

次のファイルがパッケージから抽出されます。

- {カーネルバージョン}.md5

- `splxmod-{カーネルバージョン}smp.o` (対称型マルチプロセッサの場合)
- `splxmod-{カーネルバージョン}.o` (単一プロセッサの場合)

ヒント: MD5 チェックサムを調べて、ファイルが完全な状態でダウンロードされて抽出されたことを確認することを強くお勧めします。

5. 次のコマンドを実行して ServerProtect サービスを再起動します。

```
/etc/init.d/splx restart
```

6. インストール後、次の URL から ServerProtect Web コンソールにアクセスできません。

```
http://<ホストサーバ>:14942
```

または

```
https://<ホストサーバ>:14943
```

お使いの Linux システムのポート 14942 または 14943 が開いていて、ServerProtect にアクセスできることを確認します。

カーネルフックモジュールをリモート配信する

RemoteInstall を使用して、KHM を複数のコンピュータにリモート配信できます。

RemoteInstall を使用して KHM を配信するには

1. 最新の KHM を次のトレンドマイクロ Web サイトからダウンロードします。

```
http://www.trendmicro.co.jp/download/kernel.asp?productid=20
```

2. この KHM を配信サーバ上の対応するディレクトリにコピーします。

3. RemoteInstall を実行します。

ヒント： ネットワーク全体に配信する前に、少数のコンピュータを対象にして配信をテストすることをお勧めします。

インストールを確認する

インストールが完了したら、ServerProtect が正常に動作していることを確認してください。

ServerProtect が正常に動作していることを確認するには

1. 次のコマンドをコマンドラインから実行します。

```
/etc/init.d/splx status
```

2. 次の例のように、すべての実行中プロセスが表示されます。

```
splxmod module is running...
vsapiapp (pid 3854) is running...
entity (pid 3845 3844) is running...
ServerProtect for Linux core is running...
splxhttpd (pid 3869 3868 3867 3866 3865 3864) is running...
ServerProtect for Linux httpd is running...
ServerProtect for Linux manual scan is stopped
ServerProtect for Linux scheduled scan is stopped
ServerProtect for Linux Control Manager agent is not
registered to Trend Micro Control Manager server
```

ServerProtect をアンインストールする

ServerProtect を削除するには、root でログオンしている必要があります。ターミナルウィンドウで、「rpm -e SProtectLinux」と入力して、ServerProtect サービスを停止し、アプリケーションを削除します。

インストール後の設定

本章では、Trend Micro ServerProtect for Linux (以下、ServerProtect) の Web コンソールへのアクセス方法とインストール後の設定タスクについて説明します。本章は次の内容で構成されています。

- 40 ページの「ServerProtect Web コンソールにログオンする」
- 42 ページの「管理者パスワードを設定する」
- 43 ページの「プロキシサーバを設定する」
- 46 ページの「ServerProtect を登録する」
- 47 ページの「アクティベーションを実行する」
- 49 ページの「製品版にアップグレードする」
- 51 ページの「コンポーネントをアップデートする」
- 52 ページの「EICAR テストウイルスを使用して ServerProtect をテストする」
- 53 ページの「SUSE Linux の syslog-ng を設定する」

ServerProtect Web コンソールにログオンする

Web コンソールを開くには、ブラウザウィンドウの URL アドレスフィールドに次のいずれかを入力して <Enter> キーを押します。

```
http://{ホストサーバの IP アドレス}:14942  
https://{ホストサーバの IP アドレス}:14943
```

ログオン画面がブラウザウィンドウに表示されます。

注意： Web コンソールで何も操作を行わないまま 1,200 秒 (20 分) 経過すると、自動的にログアウトします。ログアウトした場合には、パスワードを入力して [Log On] をクリックすると、Web コンソールに再びアクセスできます。タイムアウトの初期設定を変更するには、`tmsplx.xml` ファイル (`/opt/TrendMicro/SProtectLinux` フォルダ内) の Configuration グループにある `SessionTimeout` キーを変更します。詳細については、「管理者ガイド」を参照してください。

インストール後にはじめてログオンするときは、ServerProtect にアクセスするのにパスワードは不要です。[Log On] をクリックします。



図 3-1. ServerProtect Web コンソールのログオン画面

[Summary] 画面が表示されます。この画面は、Web コンソールを開いたときの初期設定表示です。ServerProtect の登録とアクティベーションを行っていない場合、この画面には、ServerProtect がまだアクティベートされていないことを示すメッセージが表示されます。

左側のメニューから選択して、ユーザインタフェース内を移動してください。

The screenshot shows the Trend Micro ServerProtect web console interface. The main content area is titled 'Summary' and includes a warning message: 'Trend Micro has extended you a 30-day grace period.' Below this, there is a section for 'System Information (2007-01-16 22:10:03)' with the following details:

- Product version: Trend Micro ServerProtect for Linux 3.0
- Platform: Intel(R) Pentium(R) 4 CPU 3.00GHz (i686)
- OS: Red Hat Enterprise Linux ES release 4 (Nahant Update 2)
- Kernel version: 2.6.9-22.EL

The 'Scan Results for Virus' section shows '0 viruses/spywares detected today.' Below this is a table with columns for 'Summary', 'Today', and 'Last 7 days':

Summary	Today	Last 7 days
Virus undecanable	0	1
Virus quarantined	0	1
Virus deleted	0	0
Virus passed	0	0
Virus cleaned	0	0
Virus renamed	0	0

The 'Scan Status' section shows:

- Real-time Scan: Enabled (Incoming files)
- Scheduled Scan: Disabled
- Manual Scan:

The 'Update Status' section includes an 'Update now' button and a table with columns for 'Component', 'Current Version', and 'Last Updated':

Component	Current Version	Last Updated
<input checked="" type="checkbox"/> Virus Pattern	3.217.00	2006-02-17 17:11:05
<input checked="" type="checkbox"/> Spyware/Grayware Pattern	37300	2006-02-17 17:11:05
<input checked="" type="checkbox"/> Scan Engine	8.1.1002	2006-02-17 17:11:05

図 3-2. ログオン後の Web コンソールの初期設定表示

注意：リアルタイム検索は初期設定で有効になっています。

Web コンソールからログオフする前に、パスワード付きの管理者アカウントをセットアップすることをお勧めします。

Java プラグインを有効にする

Java Runtime Environment (JRE) がインストールされていないか、または有効になっていない場合、ログイン画面に次のメッセージが表示されます。



図 3-3. Java Runtime Environment (JRE) がインストールされていない Mozilla ブラウザに表示されるログイン画面

Java プラグインを有効にするには、Mozilla プラグインディレクトリに移動して、Java プラグインのシンボリックリンクを作成します。次に例を示します。

```
cd /usr/lib/mozilla/plugins
ln -s ¥
> /usr/java/j2re1.4.2/plugin/i386/ns610-gcc32¥
> libjavaplugin_oji.so libjavaplugin.so
```

管理者パスワードを設定する

左側のメニューから [Administrator]→[Password] の順に選択すると、[Password] 画面が表示されます。現在のパスワードの入力、および新しいパスワードの入力と確認入力のためのフィールドが表示されます。パスワードは、32 文字以内で、アルファベット、数字 (A～Z、a～z、0～9)、およびハイフン (-) が使用できます。

はじめてログオンしたら、[Current password] フィールドを空白のままにし、[New password] フィールドと [Confirm password] フィールドに同じ情報を入力します。また、後からこの画面でパスワードを変更できます。

注意： インストール後にはじめて ServerProtect Web コンソールにログオンする際は、パスワードは空白です(初期設定のパスワードはありません)。

パスワードをコマンドラインからリセットする方法については、「管理者ガイド」で `splxmain` コマンドの `-f` オプションに関する説明を参照してください。

プロキシサーバを設定する

インターネット接続にプロキシサーバを使用している場合は、ServerProtect で次の機能におけるプロキシを設定します。

- ウイルストラッキング
- ライセンスアップデート
- コンポーネントアップデート

一般的なプロキシ設定

ウイルストラッキング機能とライセンスアップデート機能でのプロキシの設定手順は次のとおりです。

ウイルストラッキングとライセンスアップデート用にプロキシを設定するには

1. [Administration]→[Proxy Settings] の順に選択します。[General] 画面が表示されます。
2. [Use a proxy server to access the Internet] チェックボックスをオンにします。

3. [Proxy Protocol] フィールドで、[HTTP]、[SOCKS4]、または [SOCKS5] を選択します。
4. [Server name or IP address] フィールドに、プロキシサーバの IP アドレスまたはホスト名を入力します。
5. [Port] フィールドに、プロキシサーバの待機ポート番号を入力します。
6. オプションのプロキシ認証のユーザ ID とパスワードを使用している場合は、[User name] フィールドと [Password] フィールドにこれらの情報を入力します。
7. [Save] をクリックします。

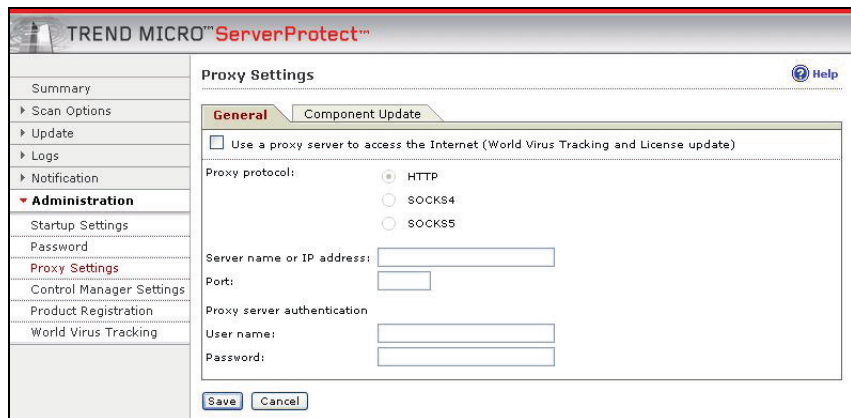


図 3-4. プロキシ設定の [General] 画面

コンポーネントアップデートでのプロキシの設定

検索エンジンとパターンファイルのアップデートに必要なプロキシサーバの設定手順は次のとおりです。

コンポーネントアップデートでプロキシを設定するには

1. [Administration]→[Proxy Settings] の順に選択します。[Component Update] 画面が表示されます。

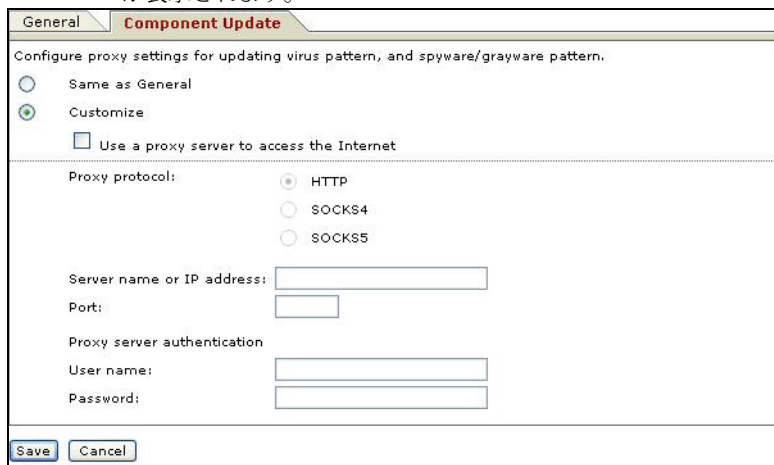


図 3-5. プロキシ設定の [Component Update] 画面

2. [General] 画面で指定したプロキシサーバの設定と同じ設定を使用するには、[Same as General] を選択します。
 - プロキシを設定するには、[Customize] を選択します。
 - コンポーネントのアップデートにプロキシサーバを使用する場合は、[Use a proxy server to access the Internet] を選択します。その後、手順 i に進みます。コンポーネントのアップデートにプロキシサーバを使用しない場合は、[Use a proxy server to access the Internet] の選択を解除します。これは、たとえば、アップデートサーバが自社のネットワーク内に存在する場合です。その後、手順 3 に進みます。
 - i. [Proxy protocol] フィールドで、[HTTP]、[SOCKS4]、または [SOCKS5] を選択します。
 - ii. [Server name or IP address] フィールドに、プロキシサーバの IP アドレスまたはホスト名を入力します。

- iii. [Port] フィールドに、プロキシサーバの待機ポート番号を入力します。
 - iv. オプションのプロキシ認証のユーザ ID とパスワードを使用している場合は、[User name] フィールドと[Password] フィールドにこれらの情報を入力します。
3. [Save] をクリックします。

ServerProtect を登録する

トレンドマイクロでは、アクティベーションコードに定められた期間内、すべての登録ユーザの皆さまに、テクニカルサポート、ウイルスパターンファイルのダウンロード、プログラムアップデートの各サービスを提供しています。期間終了後もこれらのサービスを継続してご利用になるには、サポート契約を更新していただく必要があります。

ServerProtect を登録して、最新のセキュリティアップデート、その他の製品のサービス、およびメンテナンスサービスが受けられるようにします。ServerProtect の登録は、インストール時でも、インストール後でもできます。

ServerProtect の購入時に、トレンドマイクロまたは販売代理店より、レジストレーションキーまたはシリアル番号 / アクティベーションコードを発行します。

レジストレーションキーの形式

レジストレーションキーは、次のような形式で表示されます。

XX-XXXX-XXXX-XXXX-XXXX

アクティベーションコード / シリアル番号の形式

アクティベーションコード / シリアル番号は、次のような形式で表示されます。

`XX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

注意：すでにアクティベーションコードをお持ちの場合、オンライン登録の必要はありません。

ServerProtect のアクティベーションコードをすでにお持ちの場合は、47 ページの「アクティベーションを実行する」で説明している手順に従って ServerProtect をアクティベートしてください。

レジストレーションキーをお持ちの場合には、以下の URL からオンライン登録画面にアクセスして、画面の指示に従ってアクティベーションコードを取得してください。

<https://olr.trendmicro.com/registration/jp/ja/login.aspx>

アクティベーションを実行する

ServerProtect のアクティベーションは、次のいずれかの方法で実行できます。

- インストールプロセスで実行する
- Web コンソールから [Product Registration] 画面にアクセスする
- /opt/TrendMicro/SProtectLinux/SPLX.vsapiapp フォルダで次のコマンドを入力する

```
./splxmain -q
```

ServerProtect のアクティベーションはインストール時に実行することをお勧めします。詳細については、47 ページの「アクティベーションを実行する」を参照してください。

ServerProtect を [Product Registration] 画面でアクティベートするには

1. ServerProtect Web コンソールの左側のメニューから、[Administration] → [Product Registration] の順に選択します。

2. [Activation Code] フィールドに ServerProtect のアクティベーションコードを入力します。
3. [Register] をクリックします。ServerProtect がアクティベートされます。

ServerProtect をコマンドプロンプトでアクティベートするには

1. 次のディレクトリに移動します。

```
/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp
```

2. 次のコマンドを実行すると、ServerProtect がアクティベートされます。

```
./splxmain -q <アクティベーションコード>
```

製品版にアップグレードする

インストール時に <Ctrl>+<D> キーを押して登録 / アクティベーションの手順を省略した場合、ウイルス / スパイウェアの検索、コンポーネントのアップデートなど、ServerProtect のほとんどの機能は無効になります。インストールされた製品のステータス (アクティベートされているかどうか) は、[Product Registration] 画面で確認できます。次の画面例では、ServerProtect はアクティベートされていません。

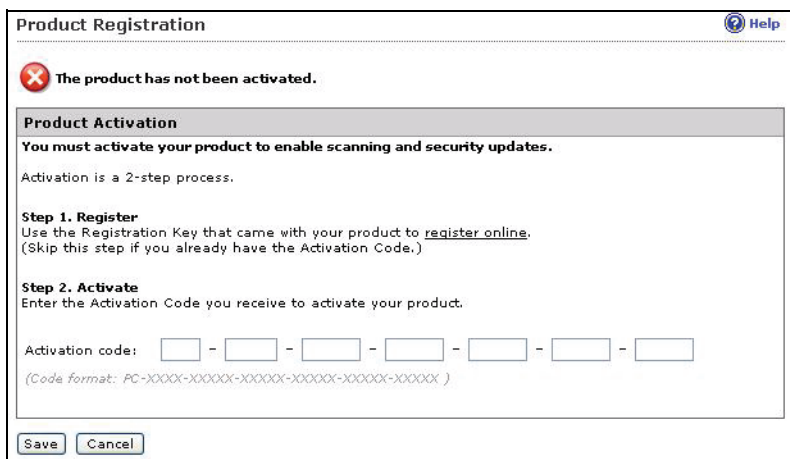


図 3-6. [Product Registration] 画面 : アクティベートされていない場合

一定の期間中、ServerProtect のすべての機能を有効にする体験版アクティベーションコードを使用している場合、[Product Registration] 画面の [Version] フィールドに「Trial」と表示されます。次はその画面例です。

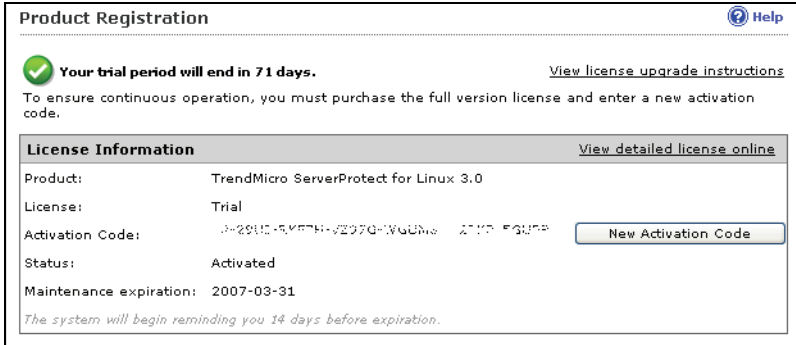


図 3-7. [Product Registration] 画面 : 体験版

ServerProtect を製品版にアップグレードするには、ServerProtect の登録とアクティベーションを実行します。ServerProtect パッケージに含まれているレジストレーションキーを使用するか、またはトレンドマイクロの販売代理店からレジストレーションキーを購入し、46 ページの「ServerProtect を登録する」で説明する手順に従って、トレンドマイクロのオンライン登録からアクティベーションコード / シリアル番号を取得します。

次は、製品版 ServerProtect の画面例です。

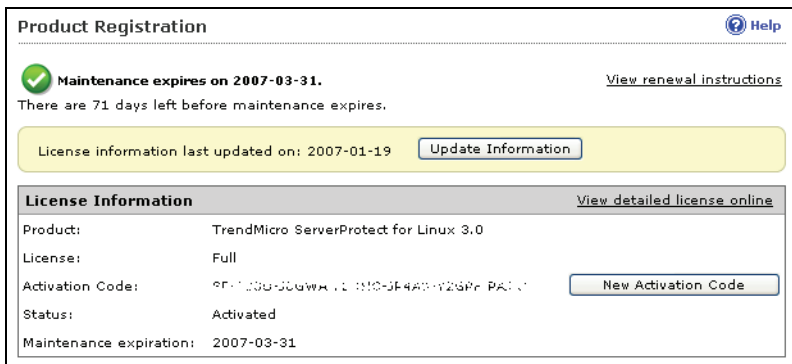


図 3-8. [Product Registration] 画面 : 製品版

コンポーネントをアップデートする

最新のウイルス / 不正プログラムやスパイウェアへの対応を確実にするため、ウイルスパターンファイル、スパイウェアパターンファイル、および検索エンジンファイルを手動または自動でアップデートしてください。

コンポーネントをアップデートするには

1. [Updata]→[Manual Update] の順に選択して [Manual Update] 画面を表示するか、または[Update]→[Scheduled Update] の順に選択して [Scheduled Update] 画面を表示します。
2. [Component] チェックボックスをオンにします。
3. [Save] をクリックします。

Control Manager による自動アップデートの開始

ServerProtect コンピュータでコンポーネントのアップデートが自動的に開始されるようにするには、Trend Micro Control Manager (以下、Control Manager) に ServerProtect を登録した後に、Control Manager サーバで設定を行う必要があります。

Control Manager から自動アップデートを開始するには

1. ServerProtect が Control Manager に正常に登録されていることを確認します。
2. Control Manager の Web コンソールにログオンし、[手動ダウンロード] 画面か [予約ダウンロード] 画面で [製品プログラム] を選択します。

Control Manager における製品の管理の詳細については、ServerProtect または Control Manager の「管理者ガイド」を参照してください。

EICAR テストウイルスを使用して ServerProtect をテストする

ServerProtect のインストール後、アプリケーションが正常に機能することを確認してください。

EICAR (European Institute for Computer Antivirus Research) は、ウイルス対策ソフトウェアをテストするためのテストウイルスを開発しました。このスクリプトは不活性テキストファイルです。このバイナリパターンは、ほとんどのウイルス対策ベンダーのウイルスパターンファイルに組み込まれています。

テストウイルスは実際のウイルスではないため、プログラムコードが含まれておらず、無害で、自己複製しません。

警告： ウイルス対策機能のテストでは、実際のウイルスを使用しないでください。

EICAR テストファイルを取得する

EICAR テストファイルは次の Web サイトからダウンロードできます。

http://www.eicar.org/anti_virus_test_file.htm

または、次の文字をテキストファイルに入力またはコピーし、拡張子が com のファイル (virus.com など) として保存します。

```
X50!P%@AP[4#PZX54 (P^) 7CC) 7} $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

ファイルをダウンロードする前に、HTTP 検索を無効にする必要があります。ネットワークに Trend Micro InterScan VirusWall がインストールされている場合、テストファイルを、メールに添付して SMTP 検索のテストや FTP/HTTP ファイル転送の確認に使用します。

どちらを選択しても、テストファイルを単にダウンロードするか作成するだけで、リアルタイム検索によってウイルスと同様に検出されます。

SUSE Linux の syslog-ng を設定する

ServerProtect が SUSE Linux Enterprise Desktop/Server 10 上にデバッグログ情報を格納できるようにするには、syslog-ng (next generation) の設定を行います。

1. `/etc/syslog-ng/` にある `syslog-ng.conf` ファイルを開いて、このファイルに次の行を追加します。

```
# this is for splx debug log

filter f_splx                                { facility(local3); };

# logs for splx debug

destination splx_debug_log { file("/var/log/splx.debug");
};

log { source(src); filter(f_splx);
      destination(splx_debug_log); };
```

2. 端末で「`/etc/init.d/syslog restart`」と入力して syslog デーモンを再起動します。
3. `tmsplx.xml` ファイルのデバッグパラメータ (`UserDebugLevel`) を 5 に設定します。
4. 「`service splx restart`」と入力して、ServerProtect を再起動します。

設定を完了すると、ServerProtect は `/var/log/` にある `splx.debug` ファイルにデバッグ情報を格納するようになります。このファイルを開いてデバッグログを参照できます。

カーネルフックモジュールの構築とインストール

本付録では、CentOS Linux システムと SUSE Linux システムでのカーネルフックモジュール (以下、KHM) の構築およびインストール方法について説明します。本付録は次の内容で構成されています。

- 56 ページの「はじめに」
- 56 ページの「要件」
- 57 ページの「インストール」

はじめに

KHM は、Trend Micro ServerProtect for Linux (以下、ServerProtect) 用のカーネルモジュールであり、リアルタイム検索機能をサポートします。カーネルモジュール構築の通常の手順と同じ手順に従って、Linux システム上に KHM を構築できます。本書には、コマンドラインの例を記載しています。

このプロセスの概要は次のとおりです。

手順 1: Linux カーネルのバージョンとアーキテクチャを調べる

手順 2: カーネルソースを準備する

手順 3: カーネルソースを設定する

手順 4: KHM を構築する

手順 5: KHM をテストする

手順 6: KHM をインストールする

手順 7: ServerProtect を再起動する

要件

KHM を正常に構築するのに必要なものは、次のとおりです。

- Linux システムへの root アクセス権
- GCC
- GNU Make
- 実行カーネルに対応するカーネルソースと設定ファイル

インストール

手順 1: Linux カーネルのバージョンとアーキテクチャを調べる

お使いの Linux システムのカーネルのバージョンを調べるには、次のコマンドを使用します。

```
uname -r
```

このコマンドは、文字列 (「2.6.9-22.ELsmp」など) を返します。本書では、「<カーネルバージョン>」をこの文字列に置き換えます。

お使いの Linux システムのカーネルのアーキテクチャを調べるには、次のコマンドを使用します。

```
uname -m
```

このコマンドは文字列 (通常、「i686」または「x86_64」) を返します。本書内では、「<アーキテクチャ>」をこの文字列に置き換えます。

ヒント: ServerProtect Web コンソールの [Summary] 画面でも、同じ情報を確認できます。

手順 2: カーネルソースを準備する

お使いの Linux システムで設定済みのカーネルソースが利用できるかどうかを確認します。このセクションでは、次の Linux システムのカーネルソースの準備方法について説明します。

- CentOS Linux
- SUSE Linux Enterprise Desktop/Server
- カスタム構築した Linux システム

どの Linux ディストリビューションを使用しているか調べるには、ServerProtect Web コンソールの [Summary] 画面をチェックするか、または `/etc/issue` ファイルを表示します。次のコマンドを実行すると、ファイルの内容が表示されます。

```
cat /etc/issue
```

CentOS Linux を使用している場合

次の RPM パッケージのいずれか 1 つがインストールされているかどうかを確認します。

- kernel-devel
- kernel-hugemem-devel
- kernel-smp-devel

注意：これらのパッケージの 1 つがすでにインストールされているかどうか確認する方法については、トラブルシューティングの「KHM の構築とインストール」#1 (67 ページ) を参照してください。

RPM パッケージをインストールするには、次のコマンドを入力します。インストールするパッケージは、実行カーネルのバージョンによって決まります。

```
rpm -ivh <rpm パッケージ名 >
```

例：

実行カーネルのバージョンが「2.6.9-5.EL」で、アーキテクチャが「i686」の場合は、次のように入力します。

```
rpm -ivh kernel-devel-2.6.9-5.EL.i686.rpm
```

実行カーネルのバージョンが「2.6.9-22.ELsmp」で、アーキテクチャが「x86_64」の場合は、次のように入力します。

```
rpm -ivh kernel-smp-devel-2.6.9-22.EL.x86_64.rpm
```

コマンドラインを使用する他に、次のいずれかを使用してパッケージをインストールすることもできます。

- Linux デスクトップ環境 (たとえば GNOME など、[Application]→[System Settings]→[Add/Remove Program] の順に選択)
- `up2date` プログラム

SUSE Linux Enterprise Server/Desktop を使用している場合

お使いの Linux システムに次の RPM パッケージがインストールされているかどうか確認します。

- `kernel-source`
- `kernel-syms`

注意：これらのパッケージの 1 つがすでにインストールされているかどうか確認する方法については、トラブルシューティングの「KHM の構築とインストール」#1(67 ページ)を参照してください。

パッケージをインストールするには、次のコマンドを入力します。

```
rpm -ivh <rpm パッケージ名 >
```

例:

実行カーネルのバージョンが「2.6.16.27-0.6-default」の場合は、次のように入力します。

```
rpm -ivh kernel-source-2.6.16.27-0.6.i586.rpm
```

```
rpm -ivh kernel-syms-2.6.16.27-0.6.i586.rpm
```

また、YaST ツールを使用してパッケージをインストールすることもできます。

自分で構築したカスタムのカーネルを使用している場合

実行カーネルのバージョンに合わせて、カーネルソースが正しく設定され、準備されているかどうか確認します。

通常、確認するには、次のように入力して、/boot ディレクトリからカーネルソースディレクトリ (/usr/src/linux-<カーネルバージョン> など) に設定ファイルをコピーし、make oldconfig コマンドと make modules_prepare コマンドを実行します。

```
cp /boot/config-<Kernel Version> /usr/src/linux-<カーネルバージョン>/.config  
  
cd /usr/src/linux-<カーネルバージョン>  
  
make oldconfig  
  
make modules_prepare
```

手順 3: カーネルソースを設定する

コンパイル後の KHM のサイズを小さくするため、カーネルの設定の [Kernel Hacking] メニューで [Compile the kernel with debug info] オプションの選択を解除することをお勧めします。

カーネルソースは次のディレクトリにあります。

```
cd /lib/modules/<カーネルバージョン>/build
```

次に、カーネルソースディレクトリで次のコマンドを入力して、設定ユーザインタフェースを表示します。

```
make menuconfig
```

[Kernel Hacking] メニューで [Compile the kernel with debug info] オプションを確認します。この項目の前にアスタリスクが表示されている場合は、キーボードの「N」を入力してアスタリスクを消去します。その後、設定ユーザインタフェースを終了して、設定を保存します。

警告： 設定ユーザインタフェースでは、[Compile the kernel with debug info] オプションのみ、選択解除します。他のオプションは変更しないでください。変更すると、KHM の使用中にカーネルパニックが発生する可能性があります。

注意： 「make menuconfig」コマンドの使用中に問題が発生した場合は、使用している Linux システムに「ncurses」パッケージがインストールされていない可能性があります。次のいずれかを実行してください。

- パッケージをインストールする。Linux インストール CD からパッケージを取得するか、Linux ベンダーの Web サイトからパッケージをダウンロードします。
- カーネルソースディレクトリにある .config ファイルを変更する。ファイル内の CONFIG_DEBUG_INFO=y を CONFIG_DEBUG_INFO=n に変更します。

設定後、次のコマンドを入力して、カーネルモジュールのコンパイルに使用するソースを準備します。

```
make modules_prepare
```

手順 4: KHM を構築する

注意： 実行カーネルのアーキテクチャが x86_64 の場合、構築プロセスが正常に終了しないときの対処法については、トラブルシューティングの「KHM の構築とインストール」#6(68 ページ)および #7(69 ページ)を参照してください。

KHM ソースが保存されているディレクトリ (初期設定の位置は /opt/TrendMicro/SProtectLinux/SPLX.module/src/module) に移動します。

`make` コマンドを使用して新しい KHM を生成します。

```
cd /opt/TrendMicro/SProtectLinux/SPLX.module/src/module
```

```
make
```

構築プロセス中に表示される警告メッセージは無視してかまいません。構築プロセスが正常に終了すると、`splxmod-<カーネルバージョン>.<アーキテクチャ>.o` というファイル名の KHM が `bin` ディレクトリに生成されます。

手順 5: KHM をテストする

注意: コンピュータに KHM をインストールする前に、この KHM テストを実行することをお勧めします。このテストにより、動作しない KHM を Linux コンピュータに誤ってインストールしてしまうのを回避できます。このような KHM をインストールすると、システムを再起動するたびにコンピュータがハングアップします。

KHM テストの実行前に、次のように入力して ServerProtect のサービスを停止します。

```
/etc/init.d/splx stop
```

次のコマンドを入力して、構築した KHM の基本機能のテストを実行します。通常、このテストは 5 秒以内に終了します。このテストが 5 秒以上かかる場合は、システムが応答していない可能性があります。

```
make test
```

警告: このテストスクリプトでは、KHM が動作可能かどうかを確認する基本テストのみが実行されます。テストが正常に終了しても、その KHM がどのような状況でも正常に動作することが保証されたわけではありません。KHM テスト中には、システムがハングアップしたり、カーネルパニックが発生したりすることがあります。そのため、このテストは、テストコンピュータで実行することをお勧めします。

次の場合の対処法については、68 ページの手順 5 を参照してください。

- KHM テスト中に Linux コンピュータが応答しなくなった
- KHM テストに失敗した (この場合は、その KHM をインストールしないでください)

手順 6: KHM をインストールする

コンパイル済み KHM のテストが正常に終了した場合は、次のインストールスクリプトを入力することによって、KHM をインストールできます。

```
make install
```

このコマンドにより、コンパイル済み KHM が `/opt/TrendMicro/SProtectLinux/SPLX.module` ディレクトリにコピーされます。このディレクトリに同名の KHM がすでに存在する場合は、元のファイルの名前の末尾に `.bak` が自動的に付加されます。

システムの再起動後、Linux コンピュータが応答しなくなった場合は、トラブルシューティングの #8 を参照してください。

手順 7: ServerProtect を再起動する

新たにインストールした KHM が使用されるように、ServerProtect を再起動します。

```
/etc/init.d/splx restart
```


トラブルシューティングとテクニカルサポート

本章では、役に立つトラブルシューティングのヒントとテクニカルサポートへの問い合わせに必要な情報について説明します。

本章では、次の内容について説明します。

- 66 ページの「トラブルシューティング」
- 71 ページの「お問い合わせいただく前に」
- 72 ページの「製品サポート情報」
- 72 ページの「サポートサービスについて」
- 73 ページの「製品 Q&A のご案内」
- 73 ページの「セキュリティ情報」
- 75 ページの「ウイルス解析サポートセンター「TrendLabs」」

トラブルシューティング

Trend Micro ServerProtect for Linux (以下、ServerProtect) の使用中に直面する可能性のある問題について、解決方法を説明します。

64 ビット SUSE Linux 上でのインストールに関連する問題

64 ビットの SUSE Linux コンピュータで linux32-Konsole を使用する場合、`insmod` エラーが発生してインストールに失敗します。この問題を解決するには、別のコンソールプログラムを使用して ServerProtect をインストールします。

Linux 内で、依存ライブラリがないことに関連する問題

Linux コンピュータに ServerProtect を正常にインストールするには、次の依存ライブラリがインストールされていなければなりません。

- `compat-libstdc++-296` (CentOS のみ)
- `gtk2`
- `pango`
- `atk`

KHM の構築とインストール

1. `make` プログラムで、カーネルソースパッケージまたはカーネルオブジェクトパッケージをインストールするように求めるプロンプトが表示されたら、どうしたらいいですか。

57 ページの「手順 2: カーネルソースを準備する」の作業が必ず正常に終了していなければなりません。必要な RPM パッケージがすでにインストールされているかどうか確認するには、次のコマンドを入力します。

```
rpm -q <rpm パッケージ名 >
```

必要なパッケージがインストールされていない場合は、Linux ベンダーの Web サイトまたはインストールソース (CD-ROM など) からパッケージを取得して、インストールします。

2. カスタム構築したカーネルを使用しています。カーネルソースは準備してありますが、「make」コマンドを入力すると、まだ「Unable to locate source package」というメッセージが表示されます。

`/usr/src/linux-< カーネルバージョン >` ディレクトリにカーネルソースをコピーするか、またはカーネルソースのシンボリックリンクを作成してから、`make` コマンドを再実行してみてください。

3. テストプログラムに「Cannot find ... symbol in System.map」というメッセージが表示されます。

KHM が正常に動作するためには、`/boot/System.map-< カーネルバージョン >` ファイルから特定のシンボルアドレスを取得する必要があります。このファイルがないと、KHM は正常に動作しません。このファイルが存在しなければ、Linux カーネルを再構築してこのファイルを取得しなければならない場合があります。

4. KHM 構築プロセスが正常に終了しない場合はどうしたらいいですか。

まず、トレンドマイクロの Web サイトにアクセスして、お使いの Linux システムに適した KHM が入手可能かどうか確認します。入手可能な場合は、その KHM をダウンロードして使用します。

トレンドマイクロでの KHM ソースコードの更新状況は、トレンドマイクロの Web サイトで確認できます。Linux カーネルは定期的に更新されているため、トレンドマイクロでも、新しい Linux カーネルに適合するように、それぞれのカーネルに対応する KHM ソースコードを定期的に更新しています。

KHM コードは GPL ベースで発行されているため、このソースコードを変更して、独自の問題解決を試みることもできます。
5. テストプログラムがクラッシュまたはハングアップした場合や、「Cannot remove KHM from kernel」というメッセージが表示された場合は、どうしたらいいですか。

まず、システムを再起動した後、トレンドマイクロの Web サイトにアクセスして、お使いの Linux システムの KHM が入手可能かどうか確認します。入手可能な場合は、その KHM をダウンロードして使用します。

トレンドマイクロでの KHM ソースコードの更新状況は、トレンドマイクロの Web サイトで確認できます。Linux カーネルは定期的に更新されているため、トレンドマイクロでも、新しい Linux カーネルに適合するように、それぞれのカーネルに対応する KHM ソースコードを定期的に更新しています。

KHM コードは GPL ベースで発行されているため、このソースコードを変更して、独自の問題解決を試みることもできます。
6. **make** プログラムで、必要な .S ソースファイルが見つからなかったことを通知する警告メッセージが表示されます (x86_64 アーキテクチャの場合のみ)。

x86_64 アーキテクチャのシステム用に KHM を構築した場合は、コンパイルプロセスで追加の 2 つの ASM ファイルが必要になります。トレンドマイクロでは、カーネルバージョン 2.6.9、2.6.16、2.6.18 用の ASM ファイルを提供しています。これら以外の実行カーネルバージョンを使用している場合は、次の手順に従って独自の ASM ファイルを作成する必要があります。

 - a. 実行カーネルのカーネルソースを確実に準備します (Red Hat Enterprise Linux の場合、kernel-devel パッケージだけでは十分ではありません)。

- b. `/opt/TrendMicro/SProtectLinux/SPLX.module/src/module/bin/kernel` ディレクトリで、`x86_64_execve_entry.<カーネルバージョン>.S` および `ia32_execve_entry.<カーネルバージョン>.S` という名前の、2つの新しいファイルを作成します。
 - c. カーネルソースディレクトリにある `arch/x86_64/kernel/entry.S` ファイルと `arch/x86_64/ia32/ia32entry.S` ファイルに基づいて、手順 b で作成したファイルにコードを入力します。`bin/kernel` KHM ソースディレクトリにある例に従って、ファイル内のコードを変更してください。
7. `make` プロセスで、`System.map` に `phys_base` と `change_page_attr_addr` が見つからないことを通知する警告メッセージが表示されます (x86_64 アーキテクチャの場合のみ)。

2.6.18 より後のカーネルバージョン (たとえば、Red Hat Enterprise Linux 5 など) では、`sys_call_table` メモリページが読み取り専用を設定されます。システムコールテーブルの属性を変更するために使用される一部の関数は、カーネルでエクスポートされません。`Makefile` のスクリプトは、2つの関数 `phys_base` と `change_page_attr_addr` のアドレスを見つけて、`bin/modreg.c` ファイルに追加しようとします。次はこのコマンドラインの例です。

```
#define PHYS_BASE 0xffffffff8034ce78
```

```
#define CHANGE_PAGE_ATTR_ADDR 0xffffffff8007dd22
```

通常、これらのアドレスは、次のコマンドを使用して、`/boot/System.map-<カーネルバージョン>` ファイルから検索できます。

```
# grep phys_base /boot/System.map-<カーネルバージョン>
```

```
# grep change_page_attr_addr /boot/System.map-<カーネルバージョン>
```

`make` プロセスで、これらのアドレスを取得できないことを通知する警告メッセージが表示された場合は、実行カーネルに対応する `System.map` ファイルが `/boot/System.map-<カーネルバージョン>` に存在するかどうか確認してください。存在しなければ、カーネルを再構築してこのファイルを取得しなければならない場合があります。

8. KHM をインストールした後、システムの再起動後に Linux コンピュータがハングアップします。
- この問題は、Linux コンピュータで正常に動作するかどうかの検証テストを行わずにインストールした KHM に原因がある可能性があります。この問題を解決するには、次の手順に従ってください。
- a. Linux コンピュータを再起動して「init 1」モードを開始します (そのためには、GRUB などのブートローダでカーネルのブートパラメータを変更します)。
 - b. 次のコマンドを入力して、`/opt/TrendMicro/SProtectLinux/SPLX.module` ディレクトリから KHM を削除します。

```
rm
/opt/TrendMicro/SProtectLinux/SPLX.module/splxmod-  
uname -r.uname -m.o
```
 - c. コンピュータを再起動します。今度は、正常に Linux システムが起動するはずですが、ただし、KHM はインストールされていないため、ServerProtect のリアルタイム検索は有効ではありません。リアルタイム検索を有効にするには、KHM を再構築します。
- この問題を回避するため、新たに構築した KHM をインストールする場合は、事前に「make test」を実行することをお勧めします。

初期設定のパスワード

ServerProtect の初期設定では、パスワードは設定されていません。ServerProtect インストール後は、すぐにパスワードを設定するようにしてください。

Web コンソールでパスワードが拒否される

Web コンソールによって、入力したパスワードが拒否される場合があります。これには、次のような理由が考えられます。

- パスワードの誤り — パスワードでは大文字と小文字が区別されます。「TREND」、「Trend」、「trend」では異なるパスワードになります。

- ServerProtect 用にカスタマイズされた Apache サーバが応答していない — `splxhttpd` のステータスを確認してください。詳細については、「管理者ガイド」を参照してください。

デバッグログ

デバッグログの詳細については、「管理者ガイド」を参照してください。ServerProtect では、次のデバッグオプションが用意されています。

- カーネルデバッグ: カーネル関連の処理に対するデバッグ
- ユーザデバッグ: ユーザ関連の処理に対するデバッグ
- Control Manager デバッグ: Trend Micro Control Manager 関連の処理に対するデバッグ

お問い合わせいただく前に

トレンドマイクロのテクニカルサポートにお問い合わせいただく前に、次のいずれかの方法で問題の解決方法が見つかるかどうかお試しくださいをお勧めします。

- ServerProtect のドキュメント: 製品付属のマニュアルやオンラインヘルプでは、ServerProtect に関する詳細な情報を提供しています。これらのドキュメントから問題の解決方法が見つかるかどうか確認してください。
- トレンドマイクロのサポートサイト: トレンドマイクロのサポートサイト (製品 Q&A) では、トレンドマイクロのすべての製品に関する最新情報を提供しています。また、サポートサイトから、製品に関するよくある質問とその回答を検索できます。トレンドマイクロの製品 Q&A サイトには、以下の URL からアクセスできます。

<http://esupport.trendmicro.co.jp/>

製品サポート情報

ServerProtect のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポート サービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意： サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

製品 Q&A

<http://esupport.trendmicro.co.jp/corporate/search.aspx>

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報をインターネットで公開しています。トレンドマイクロのセキュリティ情報 Web サイトでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

<http://www.trendmicro.co.jp/vinfo/>

管理コンソールからセキュリティ情報 Web サイトにアクセスすることもできます。セキュリティ情報 Web サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから[セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース

- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティ情報 Web サイトに定期的にアクセスして、流行中のウイルス情報など入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出 / 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。ファイルを送信いただく前に、トレンドマイクロのウイルスデータベース検索サイトにアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

<http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp>

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

http://inet.trendmicro.co.jp/esolution/attach_agreement.asp

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ)は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国、フランス、メキシコの各国センターで構成されています。24時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む1000名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

「TrendLabs」では、品質保証のISO9001:2000認定(フィリピン)、国際規格COPC-2000規格(フィリピン)、英国の国家規格ITIL: BS15000(ドイツ)、情報セキュリティマネージメントの英国規格BS7799(フィリピン)を取得しています。

ソフトウェアアップデートについて

製品リリース後に、トレンドマイクロはソフトウェアのアップデートを頻繁に行います。これによって、製品の性能を強化し、新機能を追加し、あるいは既知の問題に対応します。アップデートを発行する理由に応じて、アップデートの種類が異なります。

トレンドマイクロがリリースするアップデートの種類の詳細は次のとおりです。

- **HotFix** : HotFixは、ユーザがレポートした個別の問題に対応する回避方法やソリューションです。HotFixは特定の問題に対応し、すべてのユーザにリリースされるものではありません。WindowsのHotFixにはセットアッププログラムが含まれていますが、Windows以外のHotFixには含まれていません(通常は、プログラムのデーモンを停止して、ファイルをコピーしてインストールディレクトリの該当ファイルを上書きしてから、デーモンを再起動します)。
- **Security Patch** : Security Patchは、主にセキュリティの問題に対応するHotFixで、すべてのユーザへ配信します。WindowsのSecurity Patchには、セットアッププログラムが含まれていますが、Windows以外のPatchには一般的にセットアップスクリプトが含まれています。

- Patch : Patch は、HotFix と Security Patch の集まりで、複数のプログラムの問題を解決します。トレンドマイクロは、定期的に利用可能な Patch を作成します。Windows の Patch には、セットアッププログラムが含まれていますが、Windows 以外の Patch には一般的にセットアップスクリプトが含まれています。
- Service Pack : Service Pack は、HotFix、Patch、機能強化が統合されたもので、製品のアップグレードと見なすこともできます。Windows と Windows 以外のどちらの Service Pack にも、セットアッププログラムとセットアップスクリプトが含まれています。

リリースされた HotFix を検索する場合は、トレンドマイクロの製品 Q&A を確認してください。

<http://esupport.trendmicro.co.jp/>

トレンドマイクロの Web サイトを定期的に調べて、Patch と Service Pack をダウンロードしてください。

<http://www.trendmicro.co.jp/download/>

すべてのリリースには、製品のインストール、配置、設定に必要な情報が記載されている Readme ファイルが含まれています。HotFix、Patch、Service Pack をインストールする前に、Readme ファイルをよく読んでください。

既知の問題

ServerProtect ソフトウェアの機能には既知の問題があり、一時的に回避方法が必要になる場合があります。既知の問題は、製品に付属の Readme に記載されています。トレンドマイクロ製品の Readme は、トレンドマイクロのアップデートセンターからも入手できます。

<http://www.trendmicro.co.jp/download/>

既存の問題は、テクニカルサポートの製品 Q&A で検索できます。

<http://esupport.trendmicro.co.jp/>

注意： Readme テキストを常に確認して、インストールや性能に影響する既知の問題に関する情報、さらに特定のリリースにおける新機能、システム要件、その他のヒントなどを確認することをお勧めします。

索引

記号

/etc/init.d/splx status 37

英数字

Control Manager 15

サーバ IP アドレス 22

サーバのポート 22

製品の表示名 23

フォルダ名 23

プロキシの設定 22

Control Manager への登録 21

Control Manager、Trend Micro Control Manager を参照 15

CVS 形式のファイルを変換する 28

EICAR、「European Institute of Computer Antivirus Research」を参照 52

EICAR テストウイルス 52

European Institute of Computer Antivirus Research (EICAR) 52

HotFix 75

Java Runtime Environment (JRE) 14

Java プラグインに関する警告 42

Java プラグインの有効化 42

JRE、Java Runtime Environment (JRE) を参照 14

KDE、Konqueror Desktop Environment を参照 14

KHM、カーネルフックモジュールを参照 34

KHM.module/ 27

Konqueror Desktop Environment 14

man ページ 8

Patch 76

Quick Access コンソール 14

Readme ファイル 9

remote.install.splx 27

RemoteInstall

CVS 形式のファイルを変換する 28

オプション 33

機能 26

グループ配信 31

サブディレクトリ 27

実行後の結果ファイル 32

実行中 31

設定キー 28

抽出 27

パラメータ 33

ファイル 27

RemoteInstall 27

RemoteInstall.conf

キー 28

RemoteInstall.conf 27、28

RemoteInstall.csv 27

RemoteInstall の実行 31

Security Patch 75

ServerProtect 36

ServerProtect サービスを起動する 36

Service Pack 76

splx.debug 53

syslog-ng 53

syslog-ng.conf 53

syslog-ng の設定 53

tmsplx.xml 27

tmsplx.xml.template 27

Trend Micro Control Manager 15

TrendLabs 75

Web コンソール

アクセス 36、40

セッションタイムアウトの初期設定 40

パスワードの拒否 70

Web コンソールタイムアウトの初期設定 40

Web コンソールへのアクセス 36、40

WVTP、ウイルストラッキングプログラムを参照 25

xmldeployer 27

xmlvalidator 27

あ

アクティベーションコード 15、47

アップデートセンター 9

アンインストール 37

インストール 17

インストールの確認 37

インストールの準備

必要な情報 15

インストールの準備手順 11

インストール方法 16

リモート 26

ローカルインストール 19

ウイルス検索テスト 52

ウイルストラッキングプログラム (WVTP) 25

エンドユーザ使用許諾契約書 21

オンラインヘルプ 8

か

カーネルフックモジュール 34

KHM パッケージの抽出 35

インストール 35

リモート配信 36

管理者パスワード

使用可能な文字 42

設定 42

リセット 43

管理者パスワードの設定 42

管理者パスワードのリセット 43

既知の問題 76

クイックスタートガイド 8

グループリモート配信 31

コンポーネントのアップデート 51

さ

サービスを起動する 36

システム要件

ソフトウェア 13

ハードウェア 12

使用許諾契約書 21

初期設定のパスワード 70

シリアル番号 47

シングルリモート配信 29

製品 Q&A 9、71、76、77

製品のアクティベーション 47

製品のアクティベーションの省略 24

製品のアップグレード 49

製品のアンインストール 37

製品のオンライン登録 47

製品のテスト 52

製品のライセンス 24

製品版へのアップグレード 49

製品をアクティベートする 24

設定ファイル 26

 ConfigFilePath 28

 RemoteInstall ツールのディレクトリとファイル 27

 グループ配信 31

 シングル配信 30

 リモート配信用 28

ソフトウェアアップデート 75

 HotFix 75

 Patch 76

 Security Patch 75

 Service Pack 76

ソフトウェア要件 13

 対応 Web ブラウザ 14

 対応 X Windows デスクトップ環境 14

 対応ディストリビューションおよびカーネル 13

た

 対応 Web ブラウザ 14

 対応 X Windows デスクトップ環境 14

 対応ディストリビューションおよびカーネル 13

 テクニカルサポート 72

 テストウイルス 52

 デバッグログ

 場所 53

登録

 製品 47

 トラブルシューティング 66

は

ハードウェア要件 12

 CPU 12

 ハードディスク空き容量 12

 メモリ 12

はじめに 7

パスワード

 誤り 70

 拒否 70

 初期設定 70

プロキシサーバ 15

プロキシ設定 43

 一般的 43

 ウイルストラッキングプログラム 43

 コンポーネントのアップデート 44

プロキシの設定

 Control Manager 22

や

 有効化、Java プラグイン 42

ら

リアルタイム

 検索 41

リモートインストール 26

 KHM の配信 36

 クライアントを指定する 29

グループ配信 31

初期設定の設定ファイル 28

シングル配信 29

レジストレーションキー 46

ローカルインストール 19

ログオン

画面 42

ログオンセッションの制御 40

ログオンパスワード 42